

Switch-user Security for UNIX Computer Systems

ABSTRACT OF THE DISCLOSURE

A monitoring process for defining and detecting user-switch violations and issues in a UNIX-based computer system periodically alerts system administrators of potential security risks. The monitoring process is executed at predetermined schedules, or invoked by manual command. A set of rules is defined by the system administrator, and any user-switch instances found in the UNIX user-switch log which match any rule are flagged as violations or potential security issues, and an alert notification is issued to a specified output device, such as an email address.

10